RESPONSE

Claims Status

Claims 1-21 were originally filed in this application. A restriction requirement was issued on February 7, 2005, and in a response thereto, Applicant elected to pursue claims 1 – 18 in this application. In this current Amendment and Response, Applicant has amended claims 1 – 4, 9 , 11, 16 and 18 to further clarify the invention. Support for the amendments can be found at least in the originally filed claims. No new matter has been added.

Information Disclosure Statements

Applicant thanks the Examiner for considering the references cited in the Information Disclosure Statements received on September 17, 2001, November 26, 2001, October 3, 2002, February 3, 2003, March 24, 2003, April 21, 2003 and May 3, 2004. In addition, Applicant submitted a Seventh Supplemental Information Disclosure Statement on September 1, 2005 (prior to the mailing of the current Office Action) and requests that the references included therein be considered prior to any subsequent Office Actions.

Claim Rejections

In the current Action, claims 1 – 18 were rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent Serial No. 6,233,577 to Ramasubramani et al. ("Ramasubramani").

Applicants respectfully submit that the claims as filed (and as amended) are patentable over the cited reference.

Ramasubramani

Ramasubramani is directed generally to a centralized certificate management proxy server that "manages digital certificates for . . . thin clients" and "reserves a fixed number of free certificates signed by a certificate authority and their respective private keys in a certificate database" (Abstract). The proxy server facilitates the "obtaining [of] certificates asynchronously, apart from the tradition of obtaining certificates in local devices that normally have sufficient computing power." Col. 7, line 63 – 66. The proxy server stores the certificates in a table that includes a mapping of unique device IDs assigned to each mobile device to the subscriber ID to

which the device is assigned, thus providing access to the user's account on the proxy server using only the device ID. Col. 7 lines 1-5. The user's account is "indexed by the device ID or the subscriber ID and identified by an address identifier such as a URL" and "compris[es] user info, a certificate list, and a private key list." Col. 7 lines 10-14. As such, "[a]ll certificates in the certificate list are exclusively associated with the particular account." Col. 7 lines 22-24.

Claims 1 – 3

Independent claims 1, 2 and 3 each recite, in part, "setting access privileges to the resource for a cluster of users" and, "locate" or "locating the" "access privileges based on the device identifier, the user identifier, and the cluster" and recite, in part, "authorize" or "authorizing" "a session . . . based on the located access privileges."

As described above, Ramasubramani provides digital security certificates to users which are unique to a single user, and does not mention assigning common profile or access privileges to groups or clusters of users. In contrast, Applicants claim "locating access privileges" based on a "cluster," which typically is a group of multiple users. Because the access privileges can be attributed to a cluster of users, they are distinct from the single user-specific digital certificates of Ramasubramani.

Applicants' claims recite receiving two elements that are used to locate the appropriate access privileges: the "device identifier" (e.g., to assure the device is authentic) and the "user identifier" (e.g., to authenticate the user, confirm the user is authorized to use the device and determine the cluster to which the user belongs). See, for example, paragraphs 0043 and 0044 of Applicant's published application. As described above, Ramasubramani relies on a one-to-one mapping of device ID to user ID to locate user-specific certificates, based solely on the device ID. Ramasubramani therefore uses at most only one of those elements to locate a certificate.

The Office Action states that Ramasubramani describes receiving a request for access to a resource that includes both a device ID and a user ID, and that Ramasubramani uses both of these elements to locate access privileges. Office Action, pg. 3. The text of Ramasubramani contradicts this interpretation. As described there, when a user requests a certificate from the proxy server, "the device ID 86123456-10900 is extracted from the request and verified that there is an account indexed by the same device ID 86123456-10900." Col. 9 lines 14 – 17.

Thus, the device ID of Ramasubramani provides the only mechanism by which the proxy server locates a subscriber's account and provides access – the user ID is stored on the proxy server and accessed as a result of receiving the device ID. Ramasubramani teaches away from including the user-specific data in the request: "It should be noted that the response does not request from the user a pair of username and password to permit access to the account, in fact the permission to access the account has been granted by matching the device ID in the request from the mobile device and the stored device ID of the account in the self-provision." Col. 8 lines 43 – 50. Only after the authentication can a user provide a user ID as a separate transmission in order to update their account information and authorize access to their account information via a separate device, namely a PC. Col. 9, lines 28-36.

As such, Applicants respectfully submit that independent claims 1, 2 and 3, as well as those claims that depend therefrom, are patentable over the cited reference.

Claims 4 – 18

Independent claims 4, 11 and 18 as amended each recite, in part, locating "context information associated with the device identifier" where the context information has been "assigned to the device during a previous session between the device and the resource and including access privileges associated with a cluster of uses." By maintaining context information including cluster-based access privileges for individual connections and making that context information available in subsequent sessions, a user can move a mobile device among numerous access points without requiring re-registration to the network, while still making use of any group-level access privileges they may have acquired during a previous session.

As described above with respect to claims 1 – 3, Ramasubramani maintains user-specific digital certificates on a proxy server which are, by definition, unique to the user. As such, Applicants respectfully submit that independent claims 4, 11 and 18, as well as those claims that depend therefrom, are patentable over the cited reference.

CONCLUSION

Applicant respectfully requests that the Examiner reconsider the application and claims in light of this Response, and respectfully submit that the claims are in condition for allowance. If the Examiner believes, in his review of this Response or after further examination, a telephonic interview would expedite the favorable prosecution of the present application, the Applicant's attorney would welcome the opportunity to discuss any outstanding issues, and to work with the Examiner toward placing the application in condition for allowance.

Respectfully submitted,

Date: December 7, 2005
Reg. No. 41,059

Ira V. Heffan
Attorney for Applicants
Goodwin Procter LLP
Exchange Place
Boston, Massachusetts 02109
Customer No. 051414

Tel. No.: (617) 570-1777
Fax No.: (617) 523-1231